

CLAIMS:

Sub
a1
1. A method in a data processing system for maintaining a secure data block within said system, said method comprising the steps of:

5 establishing a block of data within said system, said block of data being associated with a particular user and a particular application;

establishing a hardware master key pair for said system, said hardware master key pair including a master private key and a master public key, said hardware master key pair being associated with said system so that said master private key is known to only said system; and

encrypting said block of data utilizing said master public key, said master private key being required to decrypt said encrypted block of data, wherein only said data processing system is capable of decrypting said encrypted block of data.

20 2. The method according to claim 1, further comprising the step of storing said encrypted block of data in a non-protected storage device.

3. The method according to claim 2, further comprising the steps of:

25 establishing an encryption device having an encryption engine and a protected storage device, said protected storage device being accessible only through said encryption engine; and

storing said hardware master key pair in said protected storage device.

4. The method according to claim 3, further comprising the step of said encryption engine encrypting said block of data utilizing said master public key stored in said protected storage device.

5. The method according to claim 4, further comprising the step of a remote data processing system executing said application.

6. The method according to claim 5, further comprising the step of establishing a browser program for accessing said application.

7. The method according to claim 6, further comprising the steps of:

said browser program initiating a session with said application;

said browser requesting said encryption device to decrypt said encrypted block of data;

in response to said request, said encryption device decrypting said encrypted block of data utilizing said master private key; and

said encryption device transmitting said decrypted block of data to said browser program.

8. The method according to claim 7, further comprising the step of said browser program transmitting said decrypted block of data to said application.

9. The method according to claim 8, wherein said step of storing said encrypted block of data in said non-protected storage further comprises the step of storing said encrypted block of data in a hard drive.

5 10. A data processing system for maintaining a secure data block within said system, comprising:

said system executing code for establishing a block of data within said system, said block of data being associated with a particular user and a particular application;

10 15 said system executing code for establishing a hardware master key pair for said system, said hardware master key pair including a master private key and a master public key, said hardware master key pair being associated with said system so that said master private key is known to only said system; and

20 said system executing code for encrypting said block of data utilizing said master public key, said master private key being required to decrypt said encrypted block of data, wherein only said data processing system is capable of decrypting said encrypted block of data.

11. The system according to claim 10, further comprising said system executing code for storing said encrypted block of data in a non-protected storage device.

12. The system according to claim 11, further comprising:

25 an encryption device having an encryption engine and a protected storage device, said protected storage device being accessible only through said encryption engine; and

said encryption device executing code for storing said hardware master key pair in said protected storage device.

13. The system according to claim 12, further comprising said encryption engine executing code for encrypting said block of data utilizing said master public key stored in said protected storage device.

14. The system according to claim 13, further comprising a remote data processing system capable of executing said application.

15. The system according to claim 14, further comprising said system executing code for establishing a browser program for accessing said application.

16. The system according to claim 15, further comprising:

said system executing code for said browser program initiating a session with said application;

said system executing code for said browser requesting said encryption device to decrypt said encrypted block of data;

in response to said request, said encryption device capable of decrypting said encrypted block of data utilizing said master private key; and

said encryption device executing code for transmitting said decrypted block of data to said browser program.

17. The system according to claim 16, further comprising said system executing code for said browser program

transmitting said decrypted block of data to said application.

18. The system according to claim 17, further comprising a hard drive for storing said encrypted block of data.

5 19. A data processing system for maintaining a secure data block within said system, comprising:

said system executing code for establishing a block of data within said system, said block of data being associated with a particular user and a particular application;

an encryption device executing code for establishing a hardware master key pair for said system, said hardware master key pair including a master private key and a master public key, said hardware master key pair being associated with said system so that said master private key is known to only said system;

said system executing code for encrypting said block of data utilizing said master public key, said master private key being required to decrypt said encrypted block of data, wherein only said data processing system is capable of
20 decrypting said encrypted block of data;

said system executing code for storing said encrypted block of data in a hard drive;

said encryption device having an encryption engine and a protected storage device, said protected storage device
25 being accessible only through said encryption engine;

said encryption device executing code for storing said hardware master key pair in said protected storage device;

said encryption engine executing code for encrypting
said block of data utilizing said master public key stored
in said protected storage device;

a remote data processing system capable of executing
said application;

said system executing code for establishing a browser program for accessing said application;

said system executing code for said browser program
initiating a session with said application;

said system executing code for said browser requesting
said encryption device to decrypt said encrypted block of
data;

in response to said request, said encryption device capable of decrypting said encrypted block of data utilizing said master private key;

said encryption device executing code for transmitting
said decrypted block of data to said browser program;

said system executing code for said browser program transmitting said decrypted block of data to said application.